L Number	Hits	Search Text	DB	Time stamp
16	72	705/69.ccls.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 15:13
17	67	705/69.ccls. and @ad<20000328	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 15:13
18	50	(705/69.ccls. and @ad<20000328) and (signatures ("more than one" adj signature))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 15:16
19	0	(705/69.ccls. and @ad<20000328) and (("more than one" adj signature))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 15:16
20	8	(705/69.ccls. and @ad<20000328) and ((many several multiple plurality two three four) adj signatures)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 15:27
21	45	(705/69.ccls. and @ad<20000328) and (verif$9 with ((all adj signatures) (each signature)))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 15:26
22	0	(705/69.ccls. and @ad<20000328) and (verif$9 with ((all adj signatures) (each adj signature)))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 15:26
23	0	@ad<20000328 and (verif$9 with ((all adj signatures) (each adj signature)))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 15:27
24	0	@ad<20000328 and (verif$9 same ((all adj signatures) (each adj signature)))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 15:27
25	0	(verif$9 same ((all adj signatures) (each adj signature)))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 15:27
26	178	(verif$9 same (((many several multiple plurality two three four) adj signatures) (each adj signature))).	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 15:27
27	178	(verif$9 same (((many several multiple plurality two three four) adj signatures) (each adj signature)))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 15:28
28	69	(verif$9 with (((many several multiple plurality two three four) adj signatures) (each adj signature)))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 15:28
29	14	((verif$9 with (((many several multiple plurality two three four) adj signatures) (each adj signature)))) and @ad<20000328 and (digital adj signature?)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/17 15:28
-	237	multiple adj signatures	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 07:57
-	0	(multiple adj signatures) same ((different distinct) with random with numbers)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 07:58
-	0	(multiple adj signatures) same (random with numbers)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 08:00

-	5	(multiple adj signatures) same (random)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 08:03
-	127	redund?nt with signature	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 08:03
-	0	(redund?nt adj signature) same message same random	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 08:03
-	780	(signature) same message same random	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 08:03
-	62	(signatures) same message? same random	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 08:11
-	1	((two multiple plurality three four five six many redund?nt) adj signatures) same message? same random	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 08:12
-	40	((two multiple plurality three four five six many redund?nt) adj signatures) same message?	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 09:44
-	109	naccache-david.in. stern-jacques.in. paillier-pascal.in.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 09:44
-	39	(naccache-david.in. stern-jacques.in. paillier-pascal.in.) and signature	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 09:55
-	8	((naccache-david.in. stern-jacques.in. paillier-pascal.in.) and signature) and dsa	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 09:54
-	1	(naccache-david.in. stern-jacques.in. paillier-pascal.in.) and (chop$5)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 09:55
-	45	(naccache-david.in. stern-jacques.in. paillier-pascal.in.) and signature	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 09:55
-	47	twin$5 same signature	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 09:55
-	6	(twin$5 same signature) and (713.clas. 380.clas. 705.clas. 708.clas.)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 10:07
-	4	(713.clas. 380.clas. 705.clas. 708.clas.) and @ad<20000328 and (sign with message with ("more than once" twice))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 10:08
-	6	probabilistic adj signature	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 15:59
-	66	@ad<20000328 and ((double dual twin pair?? duplicate) adj signature)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/12 16:07
-	28	@ad<20000328 and ((double dual twin pair??)adj signature)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 11:27

-	30	@ad<20000328 and multicasting and (digital adj signature)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 12:22
-	5	@ad<20000328 and (multi adj cast$3) and (digital adj signature) and (public) and (private)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 12:24
-	38	@ad<20000328 and (redundan$4 adj2 signature)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 12:25
-	32	(@ad<20000328 and (redundan$4 adj2 signature)) not (cyclic adj redundancy adj check)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 12:27
-	12	((@ad<20000328 and (redundan$4 adj2 signature)) not (cyclic adj redundancy adj check)) and signatures	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 12:37
-	34	signatures with ("same" with message?)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 12:40
-	1	signatures with ("same" adj message?)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 12:41
-	76	signatures with (twice)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 12:42
-	2917	signatures and (sign$3 and twice)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 12:42
-	340	signatures and (sign$3 with twice)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 12:43
-	33	signatures and (sign$3 with "same" with twice)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 12:43
-	19	(signatures and (sign$3 with "same" with twice)) and @ad<20000328	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 12:43
-	2	(("5224163") or ("5450489")).PN.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 13:20
-	238	(713/180).CCLS.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 13:21
-	1	((713/180).CCLS.) and chop$5	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 13:21
-	41	((713/180).CCLS.) and (sign$3 adj ("more than once" ((plurality many several two three four five) adj times)) twice)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 13:24
-	4	((713/180).CCLS.) and (sign$3 adj ("more than once" ((plurality many several two three four five) adj times) twice))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/08/16 13:41

Terms used **digital signature twinning dual signatures double signatures twin signatures**

Found **7** of **140,980**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 7 of 7

Relevance scale

1 Password Management and Digital Signatures: Twin signatures: an alternative to the hash-and-sign paradigm

David Naccache, David Pointcheval, Jacques Stern

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**

Full text available: pdf(402.64 KB) Additional Information: full citation, abstract, references, index terms

This paper introduces a simple alternative to the hash-and-sign paradigm, from the security point of view but for signing short messages, called *twinning*. A twin signature is obtained by signing twice a short message by a signature scheme. Analysis of the concept in different settings yields the following results:

- We prove that no generic algorithm can efficiently forge a twin DSA signature. Although generic algorithms offer a less stringent form of security than computational red ...

Keywords: digital signatures, discrete logarithm, flexible RSA problem, generic model, provable security, standard model

2 Cryptographic protocols: The verification of an industrial payment protocol: the SET purchase phase

Giampaolo Bella, Lawrence C. Paulson, Fabio Massacci

November 2002 **Proceedings of the 9th ACM conference on Computer and communications security**

Full text available: pdf(209.87 KB) Additional Information: full citation, abstract, references, citings, index terms

The Secure Electronic Transaction (SET) protocol has been proposed by a consortium of credit card companies and software corporations to secure e-commerce transactions. When the customer makes a purchase, the SET dual signature guarantees authenticity while keeping the customer's account details secret from the merchant and his choice of goods secret from the bank.This paper reports the first verification results for the complete purchase phase of SET. Using Isabelle and the inductive method, we ...

Keywords: electronic commerce, formal verification, inductive specifications, isabelle proof assistant, security protocols

3

Securing ad hoc routing protocols
Manel Guerrero Zapata, N. Asokan
September 2002 **Proceedings of the ACM workshop on Wireless security**

Full text available: pdf(258.53 KB) Additional Information: full citation, abstract, references, citings, index terms

We consider the problem of incorporating security mechanisms into routing protocols for ad hoc networks. Canned security solutions like IPSec are not applicable. We look at AODV[21] in detail and develop a security mechanism to protect its routing information. We also briefly discuss whether our techniques would also be applicable to other similar routing protocols and about how a key management scheme could be used in conjunction with the solution that we provide.

Keywords: SAODV, ad hoc wireless networks, hash chains, routing protocols, secure AODV, security

4 Summaries of MobiHoc 2003 posters: Secure routing with tamper resistant module for mobile Ad hoc networks
Joo-Han Song, Vincent Wong, Victor Leung, Yoji Kawamoto
July 2003 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 7 Issue 3

Full text available: pdf(144.05 KB) Additional Information: full citation, references

5 Constructing replicated systems using processors with point-to-point communication links
P. D. Ezhilchelvan, S. K. Shrivastava, A. Tully
April 1989 **ACM SIGARCH Computer Architecture News , Proceedings of the 16th annual international symposium on Computer architecture**, Volume 17 Issue 3

Full text available: pdf(948.34 KB) Additional Information: full citation, abstract, references, citings, index terms

Replicated processing with majority voting is a well known method of achieving fault tolerance. We consider the problem of constructing a distributed system composed of an arbitrarily large number of N-modular redundant (NMR) nodes, where each node itself is composed of N, N = 2m + 1 and m $\geqslant$ 1, processing and voting elements. Advanced microprocessors, such as Inmos Transputers, provide fast serial communication links for inter-processor communication, making it possible to construct larg ...

Keywords: N-modular redundancy, fault tolerance, majority voting, replicated processing, sequencing algorithm

6 Strong password-only authenticated key exchange
David P. Jablon
October 1996 **ACM SIGCOMM Computer Communication Review**, Volume 26 Issue 5

Full text available: pdf(1.52 MB) Additional Information: full citation, abstract, citings, index terms

A new simple password exponential key exchange method (SPEKE) is described. It belongs to an exclusive class of methods which provide authentication and key establishment over an insecure channel using only a small password, without risk of offline dictionary attack. SPEKE and the closely-related Diffie-Hellman Encrypted Key Exchange (DH-EKE) are examined in light of both known and new attacks, along with sufficient preventive constraints. Although SPEKE and DH-EKE are similar, the constraints a ...

7 Certified mail: the next challenge for secure messaging

Rolf Oppliger
August 2004 **Communications of the ACM**, Volume 47 Issue 8

Full text available: pdf(88.44 KB) html(25.71 KB) Additional Information: full citation, abstract, references, index terms

The lack of evidence for message receipt is a missing piece of the infrastructure required for the more professional use of email.

Results 1 - 7 of 7